facultatieve
GEGEVENSBESCHERMINGSEFFECTBEOORDELING (PIA) RIJKSDIENST

EOS informatieloketten

V1.0

Revisiegegevens

Versie	Datum	Auteur	Omschrijving
0.1	19-10-2017		Initiële versie obv input interviews/assessment op locatie door
0.7-0.9	23-10		Integrale uitwerking+ verwerking reviewopmerkingen collegale interviewers
1.0	15-12		Verwerking opmerkingen FG

Inhoud

I. SAMENVATTING

Een *Gegevensbeschermingseffectbeoordeling (*GEB), de nieuwe term voor een PIA, legt het vergrootglas op de verwerking van persoonsgegevens met als doel het detecteren van risico's en aanreiken van risico-verminderende maatregelen. In dit document wordt de term PIA gebruikt. Doordat het bestaande verwerkingen betreft heeft de PIA hier en daar ook het karakter van een audit gekregen.

De scope van de PIA is de verwerking van gegevensaanvragen (verzoeken, vorderingen) en daaruit voortkomende verstrekkingen en de verwerking van inkomende signalen binnen de 11 EOS fraudeloketten. Vorderingen en verzoeken om gegevens komen van zowel BD-medewerkers, medewerkers van andere overheidsinstanties. In geval van signalen betreft het andere overheidsinstanties, belastingplichtigen of anonieme personen . De resultaten zijn verzameld middels interviews gehouden door 2 personen vanuit het centrale EOS-regieteam met vertegenwoordigers van de EOS-loketten (in de meeste gevallen een TL en loket coördinator, inhoudelijk specialist/medewerker informatieloket en een (regionaal) formeel recht specialist). De interviews zijn op gestructureerde wijze vastgelegd met behulp van PAM; een proof of Concept van een Privacy Assessment Model, opgesteld door team CAP/JAG (Juridisch Advies Gegevens) en geënt op het meest recente PIA-model.

De noodzaak van de verwerkingen is voldoende aangetoond; het overgrote merendeel van de vragen correspondeert met het voldoen aan een wettelijke plicht van een andere overheidsorganisatie of betreft het zorgvuldig verwerken (incl. vernietigen) van spontaan ontvangen informatie of de eigen taken van de BD. Toetsing van de welbepaaldheid van het doel in combinatie met proportionaliteit en subsidiariteit is, hoewel niet formeel in procedures vastgelegd (aanbeveling/maatregel) overal als goed ingebedde aspecten aangetroffen.

In zijn algemeenheid is het beeld dat er binnen de loketten zorgvuldig wordt gewerkt met expliciete aandacht voor aspecten als rechtmatigheid (incl. geheimhoudingsplicht), noodzakelijkheid van de verwerking, doelbinding, proportionaliteit en subsidiariteit en informatiebeveiliging. De bevindingen die ten aanzien van voornoemde aspecten zijn gedaan hebben vooral het karakter van (eenmalige) incidenten passend bij audit-achtige karakter van een deel van de toetsing.

De bevindingen uit de interviews zijn verder vooral gedaan op het vlak informatiebeveiliging zoals de wijze van verzenden van gegevens, bewaren en vernietigen van gegevens (vaak in samenloop met het bijzondere (strafrechtelijke) karakter van de verwerkte gegevens en de (te brede) toegankelijkheid van de PIA gebruikte administraties waarin de verwerkingen (deels met (bijzondere) persoonsgegevens) staan geregistreerd.

Voor nagenoeg alle bevindingen geldt dat (een verdere) uniformering van de werkwijze middels een centraal vastgestelde werkwijze de benoemde risico's kan verminderen. Aanvullend kan door awareness, in het bijzonder voorlichting/ training het bewustzijn en 'hoe om te gaan met risico x/y/z...) leiden tot verdere verbetering. De geïnterviewde personen hebben ook duidelijk aangegeven hieraan behoefte te hebben.

II. VRAGENLIJST GEGEVENSBESCHERMINGSEFFECTBEOORDELING

A. Beschrijving algemene kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling (voorheen PIA) op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

Het onderzoeksobject van de PIA zijn de 11 EOS Informatieloketten, een belangrijke schakel in de fraude- en EOS-aanpak. De loketten zien vooral op gegevensuitwisseling met, zowel interne als externe, partners en op het ontvangen, ver- en opwerken en doorgeleiden van signalen ten behoeve van onze handhavende taken. Scope is het loket en de via het loket verwerkte gegevenstromen; bv mutaties naar aanleiding van een kliksignaal bij klantregistratie of toezicht vallen buiten scope.

2. Persoonsgegevens

Som alle categorieën persoonsgegevens op die worden verwerkt en deel ze in onder de typen: gewoon, bijzonder of strafrechtelijk en wettelijk identificatienummer. Geef per persoonsgegeven aan op wie het betrekking heeft.

Gewone persoonsgegevens
Door de informatieloketten worden persoonsgegevens verwerkt voornamelijk in combinatie/overlappend met fiscale persoonsgegevens.

In een niet limitatieve opsomming:

Bronnen			
ABS (Inkomensheffing + Vennootschapsbelasting)			
BVR- KvK-gegevens (6160)			
BVR- Ondernemingen historie (3220)			
BVR- Relaties (3150)			
BVR- Standaard NAW info (3110)			
FiBase/FLG			
GOA/DACAS + ETM en INL			
GRS (Geautomatiseerd Registratie Systeem = erf- en schenkbelasting; niet rechtstreeks benaderbaar)			
HSB– info autogegevens, lichte vrachtauto's en caravans/aanhangwagens; niet extern uitgeleverd; Rdw)			
OB			
RBG (Registratie Bankgegevens)			
BRG (Beheer Rekeningafspraak Gegevens)[1]			
RIS (Renseignementen Informatiesysteem)			
Toeslagen			
Vastgiro			
Vbn (aanslaggegevens Vennootschapsbelasting)			
WOZ			
DAS			

[1] BRG (Beheer Rekeningafspraak Gegevens) administreert bankrekeningnummers die door de Belastingdienst in het betalingsverkeer worden gebruikt

IKB/Klantbeeld Databank auto			

Registratie informatieverzoeken (incl. persoonsgegevens medewerkers en belastingplichtigen) in:
FSV (Fraude Signalering Voorziening)
Mail (medewerkers EOS loket en postbussen EOS)
Netwerkmappen (q-schijf)

Bijzondere persoonsgegevens

Veldnaam	Bron	Betrekking op
Nationaliteit en mogelijk andere bijzondere persoonsgegevens uit bijvoorbeeld een (spontaan van politie/OM ontvangen) strafdossier.	Derden; OM /Politie	Belastingplichtigen en/of (niet) beschrevenen
Gegevens van kinderen	Eigen systemen; OM /Politie	Belastingplichtigen en/of (niet) beschrevenen

Strafrechtelijke gegevens

Veldnaam	Bron	Betrekking op
Proces Verbaal	GEFIS, PVS?	Verdachten/veroordeelden
Statusinfo vervolging/opsporing	FSV	Belastingplichtigen

Wettelijk identificatienummer

Veldnaam	Bron	Betrekking op
BSN	LH	Medewerker
LH-nummer	LH	Inhoudingsplichtige
OB-nummer	OB	OB-plichtige

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.
De verwerking vindt plaats in de volgende vormen:

Hoofddoel

1.	Informatieverzoek intern Belastingdienst ogv wettelijke taak BD.
2.	Informatieverzoek derden ogv wettelijke verplichting / wettelijke taak derden zoals het voldoen aan een vordering van de OvJ op grond van art. 126nd Sv, arbeidstijdenwet, arbeid gerelateerde fraude, , uitkeringsfraude en 'ondermijnende criminaliteit'.
3.	(Klik)signalen derden verwerken; ontvangen van anonieme melders, belastingplichtigen en derde overheidspartijen.

Met opmerkingen FG Is dus ook ontvangen en niet alleen verstrekken. Discutabel: Kliks kwamen vroeger vaak voort uit rancune en bleken in de praktijk niet veel waard. Datakwaliteit en juistheid van gegevens zijn wel een verplichting: eenmaal opgeslagen onjuiste gegevens kunnen een eigen leven gaan leiden en dat geeft mega risico's voor betrokkenen. Daar zijn genoeg voorbeelden van. Wie toetst de kwaliteit van de data en HOE???

Afhankelijk van de grondslag voor de verwerking kan het een verzoek, vordering op (spontaan) signaal betreffen. De volgende verwerkingen komen voor:

Verzamelen, vastleggen, opslaan	Ja
Ordenen / Structureren	Ja
Bijwerken of wijzigen	Ja (beperkt, originele gegeven blijft bestaan vaak aangevuld met een notitie / kenmerk.
Opvragen / Raadplegen / PIAruiken	Ja
Verstrekken dmv doorzending / Verspreiden	Ja
Combineren	Ja
Afschermen	Ja
Wissen of vernietigen	Nee (of slechts ad hoc, niet centraal geregisseerd)

4. Verwerkingsdoeleinden

Beschrijf de hoofd- en nevendoeleinden van de voorgenomen gegevensverwerkingen.

Er zijn meerdere doelen voor gegevensverwerkingen binnen de scope van EOS-informatieloketten is divers.

Vanuit het perspectief van de Belastingdienst gaat het om zijn taken op het vlak van heffing en inning van belastingen en ihbz het daarmee gepaard gaande toezicht cq handhaving. (art. 8e Wbp)

Voorbeelden zijn: opsporen van strafbare feiten, het heffen van belastingen en innen van vorderingen, daarvoor noodzakelijke identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen.

Ten behoeve van externe aanvragers is het doel voldoen aan de informatieplicht jegens deze externe afnemers in het kader van hun publieke taken op gebied van toezicht, inspectie en opsporing. (art. 8c Wbp)

Voorbeelden zijn: opsporen van strafbare feiten, het heffen van premies/sociale lasten en innen van vorderingen, daarvoor noodzakelijke identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen.

Daarnaast is er een (ongestructureerde) gegevensstroom van klik/tip-signalen van natuurlijke personen ten aanzien van al dan niet beschreven belastingplichtigen die verwerkt (beoordeeld en toebedeeld) moet worden.

Met opmerkingen FG Daar hoef je niets mee te doen (geen wettelijke basis) maar daar kies je voor om iets mee te doen. Is discutabel of dat onder e past. Misschien is dit wel letter f en dat geeft aan dat hier iets wringt. In de AVG is zo'n doel nadrukkelijk uitgesloten van letter f. Risico!!!

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger.

Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Belastingdienstonderdelen	**Rol**	**Functionarissen**
Min.v.Financiën/ DG Belastingdienst	*Verwerkingsverantwoordelijke*	
BD-MKB	*Ontvangen, leveren, intern bewerken*	*Administratief medewerker informatieloket*
BD-PDB	*Ontvangen, leveren, intern bewerken*	*Administratief medewerker informatieloket*
BD- Douane	*Ontvangen, leveren, intern bewerken*	*Administratief medewerker informatieloket*
BD- Toeslagen	*Ontvangen, leveren, intern bewerken*	*Administratief medewerker informatieloket*
BD-CAP	*Ontvangen, leveren, intern bewerken*	*Administratief medewerker informatieloket*
FIOD	*Ontvangen, leveren, intern bewerken*	*Administratief medewerker informatieloket*
BD-ZGO	*Ontvangen, leveren, intern bewerken*	*Administratief medewerker informatieloket*
BD-overig	*Ontvangen, leveren, intern bewerken*	*Administratief medewerker informatieloket*
Externe partijen/samenwerkingsverbanden (grondslag art. 8 c Wbp)	***Rol***	***Functionarissen***
BIBOB	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
Track	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
iSZW	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
Politie (126n..Sv	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
Gemeenten 64 Ppw	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
iCOV	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
UWV 54 Suwi	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
RIEC-partners	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
LSI	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
LBIO	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*

ILT	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*
IND	*Verantwoordelijke+ontvanger en leveren*	*Adminstratief medewerker, specialist, analist, beheerder*

Met opmerkingen FG Zou fijn zijn als het wetsartikel waar staat dat dit moet ook wordt meegenomen.

6. Belangen bij de gegevensverwerking

Beschrijf olle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.
Het belang van de gegevensverwerking is financieel van aard: toetsing van nakomen en rechtmatigheid van financiële aanspraken / - verplichtingen en heeft betrekking op nationale/openbare veiligheid in geval van fraudepreventie/detectie. De wettelijke taken van de individuele gegevensaanvragers incl. de Belastingdienst zelf onderbouwen de noodzakelijkheid.

Met opmerkingen FG Hier staat niet het belang maar het doel. Belang geef je aan door aan te tonen dat de verwerking noodzakelijk is tov het doel. Wat gaat er mis als je dit niet doet? Waarom kan het niet anders en moet het zo??

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

De verwerking van de persoonsgegevens vindt in Nederland plaats. Wel worden er casusgewijs gegevens geplaatst binnen de RIEC-fileshare omgeving. (**uitzoekpunt; vermoedelijk** overheids-cloud in NL binnen politieomgeving).

Met opmerkingen FG Dat kan zo niet. Je moet weten waar je de gegevens heen stuurt. Is een risico.

8. Technieken en methoden van de gegevensverwerkingen incl. informatiebeveiliging

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-) geautomatiseerde besluitvorming, profilering of big dataverwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

De verwerking vindt vraaggestuurd plaats en heeft geen massaal (volume en/of 'standaard' herhalend) karakter. De informatieloketten verwerken aanvragen betreffende 1 tm maximaal 25 personen. Aanvragen die deze bandbreedte overstijgen worden in principe of afgewezen of met mededekenen van een TL of PlvDir verwerkt. In een enkel geval blijkt de mogelijkheid tot verwerking buiten de bandbreedte gemandateerd te zijn aan de loketmedewerkers zelf.

Met opmerkingen FG Goed zo!

Met opmerkingen FG Niet goed.

Gegevensvragen worden na (marginale; een vordering van de OvJ kan bv. eigenlijk ook marginaal getoetst worden) toetsing op rechtmatigheid óf direct ('handmatig') beantwoord door een loketmedewerker die zelf de gevraagde informatie opzoekt in de gevraagde systemen óf worden centraal verwerkt door EOS team Eindhoven met behulp van een zgn. 'informatiesjabloon' dat door de loketten waar de vraag is binnengekomen wordt ingevuld en aan EOS Eindhoven wordt aangeboden (en retour ontvangen voor verzending). De aanvragen worden verwerkt met behulp van een set (standaard) queries, uitgevoerd door CAP/Gegevens, die uit de bevraagde informatiesystemen de gevraagde gegevens als aanvraag registreert (audittrail) verzamelt en bij elkaar brengt.

Registratie verwerkingen:

Aanvraag en verwerkingsinformatie wordt op verschillende manieren en locaties geregistreerd; veelal in een beveiligde map op de Q-schijf, (EOS)mailpostbussen en persoonlijke mailboxen, maar ook in systemen die voor een veel bredere doelgroep dan de EOS-loketten toegankelijk zijn zoals FSV (waartoe 2500-4000 BD medewerkers toegang hebben). De need-to-know-toegankelijkheid van de EOS-verwerkingen kan hierdoor onvoldoende worden gegarandeerd. Zo kan een baliemedewerker ook zien wat voor signalen er over een belastingplichtige zijn binnengekomen.

Met opmerkingen FG Dat moet dan wel een erg betrouwbare baliemedewerker zijn die gelogd en gemonitord wordt. Hoop ik.

Informatiebeveiliging:

De gegevens worden qua verzending voornamelijk via mail verwerkt, zowel intern Belastingdienst en bij verzending naar derde partijen. Daarbij wordt niet op alle locaties en niet door iedereen gewerkt met de zgn. RER-lijst en het principe overdracht via 'BFT (Aspera, file transfer of een gegevenskluis en mail alleen als restoplossing voor partijen die op de RER-lijst staan). In het merendeel van de genoemde voorbeelden betrof het mailen aan derden die niet op de RER-lijst staan. In een aantal gevallen wordt binnen de opgesomde mogelijkheden geen werkende/werkbare bevonden oplossing gevonden en wordt overgegaan tot levering op papier per post die naar de letter van de wet 'veilig' is maar mogelijk feitelijk een groter risico vormt dan bv. mailen met een partij buiten de RER-lijst.

Er worden casusgewijs gegevens geplaatst binnen de RIEC-fileshare omgeving. (uitzoekpunt; vermoedelijk overheids-cloud in NL binnen politieomgeving).

Met opmerkingen FG Mogelijk datalek. Check beleid in HBB? BIR etc etc.

Er worden (incidenteel) gegevens ontvangen op fysieke media; veelal betreft dit anonieme tips/kliks op cd rom of usb stick. Deze gegevensdragers worden vlg de geinterviewden via EDP-auditmedewerkers / toepassingsbeheer verwerkt op daarvoor beveiligde hardware (stand-alone machine). De (onduidelijke) aard/herkomst van dergelijke media leidt per definitie tot een risicovolle vorm van gegevensverwerking.

Met opmerkingen FG Goed zo! Eigenlijk zou je hier niets mee moeten willen. Superlinke soep. Voer voor advocaten!!

9. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.

BIBOB	Wet BIBOB
DUO	WSf, Wet op het onderwijstoezicht
iSZW	Arbeidstijdenwet, Wet arbeid vreemdelingen, de Wet minimumloon en minimumvakantiebijslag en de Wet allocatie arbeidskrachten door intermediairs , de Arbeidsomstandighedenwet en de Arbeidstijdenwet (ter bevordering van veilige en gezonde werkomstandigheden en werk- en rusttijden voor werknemers), Wet economische delicten
Politie	Sectorale wetgeving strafrecht (ihbz art. 126n..Sv)
Gemeenten	Invorderingswet, Participatiewet (art. 64 Ppw)
iCOV	(sectorale) wetgeving deelnemers, geen eigen grondslag; convenant
UWV	Art. 54 Wet Suwi
RIEC-partners	Sectorale wetgeving deelnemers; convenant
LSI	Sectorale wetgeving deelnemers; convenant
LBIO	Art. 23 Wet LBio (art. 23)
ILT	Sectorale wetgeving ILT
IND	art. 107 lid 7 Vreemdelingenwet

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkings-doeleinden.
Er is geen uniforme specifiek op de EOS-loketten toegespitste werkwijze tav de te hanteren bewaar, archiverings en vernietigtermijnen. In zijn algemeenheid gelden de selectielijsten die zich, ten dele gedetailleerd, uitspreken over te hanteren termijnen. Per locatie is een verschillende werkwijze geconstateerd en op enkele lokaties zijn (lokale) instructies gemaakt

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.
Vanuit de Wbp bezien is de verwerkingsgrondslag voor de BD en de derde partijen te baseren op de respectievelijke publiekrechtelijke taken (art. 8 sub e Wbp respectievelijk art. 8 sub c Wbp).

Voor de BD gaat het om de Awr en de belastingmiddelspecificieke wetgeving.

Voor de aanvragende partijen is de wettelijke grondslag te vinden in de wetgeving zoals vermeld onder .9.

Iedere aanvraag wordt gecontroleerd op de specifieke wettelijke grondslag die de rechtmatigheid en noodzaak van de verwerking onderbouwt. Afgezien van het risico van het alleen marginaal toetsbaar zijn van bepaalde aanvragen, is overal geconstateerd dat alleen bij voldoende, expliciete kenbaarheid van de grondslag, gegevens worden geleverd (meer algemeen: gegevens worden verwerkt). Bij twijfel wordt of niet geleverd en/of overleg gevoerd met de aanvragende partij om te komen tot een nadere aanscherping.

Met opmerkingen FG Hoe en door wie en is daar bewijs van?

12. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.

Het gebruik van het BSN is voor de Belastingdienst op basis van de Awr en art. 10 van de Wet Algemene Bepalingen Burgerservicenummer) toegestaan.

Het verwerken van strafrechtelijke informatie is min of meer onlosmakelijk verbonden met het verwerken van gegevensleveringen, verzoeken/vorderingen van partijen uit de strafrechtketen zoals OM en Politie. De verwerking is in alle besproken situaties terug te brengen tot een wettelijke grondslag gekoppeld aan een uitzonderingsgrond om het te verwerken (incl. de nader uit te werken optie van vernietigen na ontvangst vanwege gebeken onbruikbaarheid). De geïnterviewde medewerkers zijn zich bewust van de noodzaak tot (extra) zorgvuldigheid die dit met zich meebrengt.

Met opmerkingen FG AVG ander regime voor strafrechtelijke gegevens dan Wbp. Soepeler! Is de WPG hier nvt??

Met opmerkingen 18-20 Wpg: http://www.legalintelligence.com/documents/1725171?srcfrm=basic+search&docindex=1&stext=Wpg&nsp=true

De noodzaak / grondslag voor de verwerking van gegevens in een ('spontaan') ontvangen proces verbaal vanuit OM/Politie moet gevalsgewijs onderzocht worden. Hiervoor bestaan op dit moment geen uniforme richtlijnen.

In de verwerkte gegevens bevinden zich mogelijk ook VIP-s en ambtenarenposten. Hiervoor bestaan op dit moment geen uniforme richtlijnen.

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

De gegevensverwerking door de informatieloketten raakt aan de BD-taken op het vlak van heffen en innen van belastingen en bijbehorend(e) handhaving en toezicht (incl. verwerking (klik)signalen of aan het voldoen van een wettelijke informateplicht jegens andere overheidsinstanties.

De in de interviews geconstateerde casusgewijze beoordeling van de aanvragen op (onder andere) doelbinding is een goede risicobeperkende maatregel. Bij een onderzoek naar bijstandsfraude is aangevraagde info bijvoorbeeld over de OB niet zondermeer passend en wordt niet of alleen na aanvullende toetsing geleverd. Sommige leveringen kunnen zoals eerder gesteld alleen marginaal getoetst worden zoals een vordering ogv art. 126 nd Sv. Tips en kliks vormen een aparte categorie waarvan mede in relatie tot bewaren/vernietigen informatie mogelijk qua (verdere) verwerking een risico vormen.

14. Noodzaak en evenredigheid

Beoordeeld of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de nagestreefde doeleinden. Ga hierbij in ieder geval in op:

a) *Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?*
De interviews hebben als algemeen beeld opgeleverd dat iedere aanvraag getoetst wordt ten aanzien van dit aspect en waar nodig wordt teruggebracht tot aanvaardbare proporties of evt. zelfs wordt afgewezen.

b) *Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?*
De interviews hebben als algemeen beeld opgeleverd dat iedere aanvraag getoetst wordt ten aanzien van dit aspect. Niet leveren komt voor, veelal vanuit proportionaliteitsoverwegingen maar ook doordat gegevens bij een bronhouder (bv basisregistratie elders) moeten worden gevraagd en niet gemakshalve in een keer bij de BD. Alternatief zou ook kunnen zijn het vragen van gegevens bij betrokkenen of administratieplichtigen zelf. Dit is niet reeeel doordat betrokkene of nog niet op de hoogte (mogen) zijn van een (voor)onderzoek en/of er specifiek behoefte is aan kwalitatief volwaardige contra-informatie. De Belastingdienst is dan een van partijen die als (authentieke) bronhouder over de gevraagde gegevens beschikt. Ten aanzien van de wijze van verwerken (zie bv. onder beveiliging de risico's benoemd mbt email-verkeer) zijn er wel bevindingen gedaan ten aanzien van het onvoldoende bekend zijn van veiligere alternatieven voor de wijze van verwerken.

Met opmerkingen FG Evidence?? Verslagen van de interviews? Ander onderzoek?

15. Rechten van de betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.

De invulling van het inzage en correctierecht en het 'vergeetrecht' kent de zelfde tekortkomingen die BD-breed bestaan ten aanzien van opzet, bestaan en werking van voorzieningen op dit vlak en is verder buiten buiten scope geplaatst van dit assessment.

Met opmerkingen FG Is dus ook niet OK.

In zijn algemeenheid is de verwerking van gegevens binnen de loketten terug te vinden in de meldingenlijst zoals gedaan aan de AP. Of de uitzonderingen op de informatieplicht (art. 23 lid 1 Avg (letters c, d, e, h) van toepassing zijn, behoeft nader onderzoek. Opname in het verwerkingenregister cfrm de AVG wordt aanbevolen.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

16. Risico's

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op:

a. *welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van betrokkene;*
b. *de oorsprong van deze gevolgen;*

c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en
d. de ernst (impact) van deze gevolgen voor de betrokkene wanneer deze intreden.
Hou bij elk aspect rekening met de aard, omvang, context en doelen van de gegevensverwerking.

1. **Rechtmatigheid en noodzaak van verwerking**
   Door de casusgewijze controle door daarin gespecialiseerde medewerkers van externe verzoeken tot verwerking door het loket is het risico voor betrokkene beperkt / aanvaardbaar. Voor interne opvragingen (incidenteel) lijkt de toetsing minder diepgravend door de interne, veelal collegiale, herkomst. Dit levert wel een risico op van onrechtmatige verwerking (huizenprijs uit kadaster bij koop woning opvragen). Tevens bestaat het risico van vermenging van rollen, bv. in geval van een iCOV opvraag door het RIEC die bij de BD-district coördinator terechtkomt.

2. **Doelbinding**
   De casusgewijze verwerking brengt een individuele toetsmogelijkheid tav doelbinding met zich mee. De EOS-medewerkers worden niet ondersteund door centrale instructies, standaard data-sets per 3e partij etc. Hierdoor ontstaat het risico van niet-uniforme verwerking en verwerking buiten de doelbinding. Tevens is niet centraal voorzien in een (standaard) disclaimer.

3. **Proportionaliteit en subsidiariteit**

   De casusgewijze verwerking brengt een individuele toetsmogelijkheid tav proportionaliteit en subsidiariteit met zich mee. De EOS-medewerkers worden niet ondersteund door centrale instructies, standaard data-sets per 3e partij etc. Hierdoor ontstaat het risico van niet-uniforme verwerking en een bovenmatige verwerking. Bij LBIO aanvragen lijkt dit zich in het bijzonder voor te doen; er worden volledige aangiften opgevraagd en geleverd.

4. **Informatiebeveiliging**
   De meeste bevindingen en daaruit voortvloeiende risico's zijn binnen dit aspect gedaan/geconstateerd. De wijze van verzenden, in het bijzonder via mail, vormt een risico zeker als niet bewust wordt omgegaan met de lijst met partijen met wie fiscale persoonsgegevens per mail gewisseld mogen worden. Daarnaast is mail een 'restvoorziening' na andere 'voorkeurs'-verzendvormen zoals BFT. Dit leidt tot het risico van onrechtmatige verwerking waaronder het specifieke risico van data-lekken. Het assessment op locatie heeft hierin qua bewustzijn al verbetering PIAracht, maar dit risico kan verder verkleind worden door aanvullende maatregelen.
   De toegang tot de (leverings)registraties behorende bij de EOS-loketten is te ruim toegankelijk met als risico kennisname van (strafrechtelijke) persoonsgegevens buiten de kring van geautoriseerde personen (need to know); dit speelt in het bijzonder bij FSV als registratietool. Dit risico is aanzienlijk te verkleinen door het implementeren van een verbeterde, uniforme werkwijze. Het aantal administraties en de mogelijke varianten vormt een 2e vergelijkbaar risico. Ook hier geldt dat uniformering het risico helpt beperken. Er zijn ongeveer 4.000 autorisaties voor FSV afgegeven in verschillende autorisaties/toegangen (van senior gebruiker tot alleen inkijk). Duidelijk is wel dat er geen automatische intrekking van autorisaties plaatsvindt en dit niet gekoppeld is met de procedure rondom IMS profielen.

Met opmerkingen FG Dit noem je m.i. een datalek en moet je asap dichtzetten. Schakel even met voor advies.

5. **Gegevenskwaliteit (waaronder data integriteit)**
   De kwaliteit van de verstrekte (fiscale) persoonsgegevens is goed. De informatie wordt als een kopie van het origineel (authentieke) gegeven verstrekt.

   De wijze van vastleggen van de verwerking (incl. persoonsgegevens) vormt wel een risico doordat de verwerking niet uniform gebeurt en vastlegging of niet of meervoudig met verschillen per locatie plaatsvindt. Bij het reconstrueren van een verwerking bv op basis van een inzageverzoek, zal dit verschillende resultaten per locatie opleveren. Ook hier geldt dat uniformering het risico helpt beperken.

6. **Data Governance (control, beheer, bewaren en vernietigen)**
   Het zicht op de verwerkingen, kwantitatief en kwalitatief kan worden verbeterd. Het aantal, per locatie verschillende, registraties vormt een risico. Ook hier geldt dat uniformering het risico helpt beperken.

7. **Awareness gebruikers**
   Het assessment op locatie heeft hierin qua bewustzijn al verbetering gebracht maar dit risico kan verder verkleind worden door aanvullende maatregelen zoals voorlichting en centraal opgestelde werkinstructies (en controle op naleving).

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van betrokkene aan te pakken.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

1. **Rechtmatigheid en noodzaak van verwerking**
   a) Herkenning rechtmatigheid uitvrager nader uniformeren,
   b) Als een interne medewerker een uitvraag doet (overigens sporadisch) vindt niet de check plaats of deze medewerker hiertoe bevoegd is. Maatregel is: check
   c) Een verstrekking van ICOV in RIEC verband komt bij de districtcoördinator (van BD) terecht. Maak hierover (aanvullende) procedure-afspraken.
   d) Borg dat politie niet ook een aanvraag doet ogv 126nd Sv bij ICOV en de FIOD-infodesk.

2. **Doelbinding**
   a) Disclaimer doelbinding / (niet) verdere verwerking centraal formuleren en altijd meeleveren.
   b) Introduceer standaard informatiesets voor (in ieder geval) veelvoorkomende, repeterende vragen. (instructie + vooringevuld informatiesjabloon)

3. **Proportionaliteit en subsidiariteit**
   a) Heroverweeg lokaal afgegeven mandaat door de TL aan de coordinator en mdw loket om akkoord te geven op "bulkaanvragen" vanuit de RIEC. Dat doorkruist de functiescheiding die hiervoor bewust is aanPIAracht.
   b) Voer een WMK toets uit op de verwerkingen voor LBIO en neem vervolgactie obv de uitkomst (gestart).

4. **Informatiebeveiliging**

   a) Maak standaard verzend'volgorde' kenbaar: 1. BFT 2. RER lijst 3. Brief 4. Restcategorie
   b) Navraag doen bij het LIEC wie geautoriseerd zijn voor RIEC IS?
      Minimale vastlegging voor login in bepaald systeem adviseren. Wat en hoe te loggen en monitoren daarvan (functiescheiding).
   c) Geen verzoeken en antwoord BD meer in FSV opnemen vanwege het raadpleegbaar zijn door bv baliemedewerkers. Maar waar dan registreren?
   d) Keuze maken mbt LBIO verzoeken mbt centraal/decentraal beleggen (WMK LBIO gestart).
   e) Werken met (voorgedefinieerde) mappenstructuur vs Connect People CP: dat gaan we niet meer PIAruiken dus? voor vastlegging verwerkte casusinfo

a. Functiescheiding
b. kantoor Utrecht verstrekt info via mailadres betreffende medewerker en niet via mailadres infoloket. Aanvraag komt wel zo binnen.

f) Logging en monitoring en bv. een meer fijnmazige (IMS)autorisatie-toekenning kan bijdragen aan een verbeterd toezicht op ongeautoriseerde toegang. Dit werkt niet voor alle PIAruikte systemen. Stoppen met PIAruik van bv. FSV is ook een maatregel (en op 1 locatie vanwege het risico ook toegepast.)

5. **Gegevenskwaliteit (waaronder data integriteit)**
   a) Mailen persoonsonafhankelijk maken (postbusverzending ipv uit persoonlijke mail).
   b) Uniformeren registratie: Op meerdere lokaties zijn er minimaal 3-4 registraties waar (deels) eenzelfde registratie van signalen en/of infoverzoeken plaatsvindt.
   c) Niet in alle gevallen wordt de geleverde info die via RIEC-IS wordt gedeeld, ook geregistreerd binnen de BD. Moeten we zowel in IS als bij BD registreren.
   d) verstrekte informatie in casusoverleg wordt niet vastgelegd. Verbeter en uniformeer dit.

6. **Data Governance (control, beheer, bewaren en vernietigen)**

   Met opmerkingen FG : Relatie met: Data management forum??/ IV&D??

   a) Centraal opstellen van een instructie vernietiging

   b) Uniformeren registratie: Op meerdere lokaties zijn er minimaal 3-4 registraties waar (deels) eenzelfde registratie van signalen en/of infoverzoeken plaatsvindt. Voorbeeld mappenstructuur uit Groningen 'omarmen'?

7. **Uniforme werkwijze incl. awareness PIAruikers**
   a) De roep is sterk om een landelijke instructie (eigenlijk meer sturing) voor de informatieloketten, al was het maar als richtlijn. Dat alles tbv (meer) eenduidigheid in werken. Hierin komt ook weer het vraagstuk centraal/decentraal naar voren. Procesplaat en AO beschrijving.

   Met opmerkingen FG Idem als vorige opm: DMF en IV&D moeten hier m.i. de kaders voor (helpen) maken.

   b) - de VTA FR gaf aan dat in een instructie uit 2015 (zie bijlage) vermeld staat dat de BIBOB-verzoeken vanuit het LBB (en route vice versa) via EHI zouden lopen....vraag is....is dat nog actueel?
   c) Synchroniseer de EOS-loketten met de FIOD infodesk qua rolverdeling, werkwijze.
   d) de OPO-tool wordt in R'dam gezien als (deels) een verlengstuk van het Informatieloket. Hier worden ook (icm FSV) signalen in vastgelegd. Maak een keuze mbt (uniform) PIAruik.
   e) Info verzoeken vanuit de rompteams worden mondjesmaat ontvangen (bijv KvK, kadaster e.d.) maar afspraak in Arnhem is dat het informatieloket daar niet van is. N.a.v. deze toets gaat dat nog eens worden aangescherpt. Maak een keuze mbt (uniforme) werkwijze.
   f) In beeld brengen bestaande SG groepen op autorisaties en benoemen SG groep.

Overig (niet zondermeer/exclusief privacy, meer werkwijze)

- een kwalitatieve check op wat voor informatie verstrekt wordt vindt niet plaats, dus meer verstrekken.
- eveneens geldt dit voor een steekproefsgewijze check op wat voor informatie verstrekt wordt.
- opgemerkt wordt dat het informatiesjabloon ook door medewerkers van de romp ?? wordt PIAruikt. Welke risico's spelen hierbij?
- Breda doet het advies om 1 infoloket in te richten voor in- en uitgaande signalen. Denk hierbij bv aan kliks. Niet verder over doorgepraat hoe men dit exact voor ogen ziet. Kan in een latere fase nog wel.
- T.a.v. de doelbinding (13) > Wat is bulk/massaal? Landelijk te voeren discussie.

Bijlage 1: Risico-score obv PAM (Proof of Concept Privacy Assessment Model CAP/JAG)

Toets-item	Risico?	Risicoscore
1. Beschrijving algemene kenmerken gegevensverwerkingen	Basisinvulling OK?	
	Opdrachtgeverschap	
2. Persoonsgegevens	Bijzondere persoonsgegevens	
	BSN verwerkt	
	Medewerkergegevens	
	Fiscale gegevens	
3. Gegevensverwerkingen	Toelichting ok?	
	Onderbouwing ok?	
4. Verwerkingsdoelen	Doeleinden OK?	
5. Betrokken partijen	Betrokken partijen ingevuld.	
	Betrokkenheid meerdere (ook externe)partijen	
	Rollen verwerkende partijen zijn duidelijk.	
	Functionarissen verwerkende partijen zijn duidelijk.	
	Er worden gegevens verwerkt van/voor partijen waarmee geen afspraken zijn gemaakt.	
6. Belangen bij de gegevensverwerking	Belangen zijn ingevuld.	
	Er zijn geen onbekende belangen opgevoerd.	
7. Verwerkingslocaties	Locaties zijn ingevuld voor BD-onderdelen.	
	Verwerking vindt binnen de BD infra plaats.	1
	Externe locaties zijn niet ingevuld.	
	Risico ten aanzien van verwerking buiten EU/EER	
8. Techniek van gegevensverwerking	Gegevens techniek van verwerking zijn ingevuld.	
	Er zijn beveiligingsrisico's mbt cloud, big data, profilering etc.	
	Er zijn beveiligingsrisico's vanwege de gehanteerde werkwijze	
	Er is geen sprake van profiling	
	Gegevens worden niet PIAruikt voor geautomatiseerde besluitvorming.	

Met opmerkingen FG Niet toch. Las ik.

	Gegevens kunnen PIAruikt worden voor identiteitsfraude.	
	Risico(s) ten aanzien van niet/onvoldoende logging en/of monitoring.	
9. Juridisch en beleidsmatig kader	Het juridisch kader voor interne verwerkingen is ingevuld.	
	Het juridisch kader voor verwerkingen door derden is ingevuld.	
10. Bewaartermijnen	Er is voldoende duidelijkheid mbt bewaartermijnen, oa door aanwezigheid selectielijsten.	
	Er is onvoldoende duidelijkheid over het aantoonbaar en tijdig vernietigen.	
11. Wettelijke grondslag	Rechtsgrond interne verwerking vormt geen risico.	
	Wettelijk grondslag externe verwerking vormt geen risico.	
12. Bijzondere persoonsgegevens	Verwerking van bijzonder persoongsgegeven.	
	Verwerking BSN als bijzonder persoongsgegeven. Verwerking toegestaan/verplicht.	
13. Doelbinding	Aan de eisen van doelbinding is niet voldaan.	
14. Noodzaak en evenredigheid	Aan de eisen van proportionaliteit is niet voldoende voldaan.	
	Aan de eisen van subsidiariteit is voldaan.	
15. Rechten betrokkenen	Aan de rechten van betrokkenen is onvoldoende invulling gegeven.	
<EINDE pagina>		

Met opmerkingen FG Ingevuld wil niet zeggen dat het ook afdoende is.